Prof. Dr. Eva Viehmann
Dr. Paul Ziegler

Introduction to Algebraic Number Theory
Sheet 6

Exercise 1. In this exercise you will prove the following result:

Theorem (Lagrange). Every natural number can be written as the sum of four squares.

(a) Use Euler's identity

$$(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2) =$$
$$(aA-bB-cC-dD)^2+(aB+bA+cD-dC)^2+(aC-bD+cA+dB)^2+(aD+bC-cB+dA)^2$$

to show that it suffices to prove the theorem for odd prime numbers p.

(b) Show that the congruence $m^2+n^2+1 \equiv 0 \pmod p$ has a solution $(m,n) \in \mathbb{Z}^2$. For this consider the number of residue classes mod p which contain a square respectively a number of the form n^2+1.

(c) For m,n as above let $\Gamma \subset \mathbb{Z}^4$ be the set of (a,b,c,d) which satisfy

$$c \equiv ma+nb,\ d \equiv mb-na \pmod p.$$

Show that $\Gamma \setminus \{0\}$ contains a point of norm $< \sqrt{2p}$.

(d) Use a)-c) to prove the theorem.

Exercise 2. For a number field K, show that the sign of the discriminant $d_K \in \mathbb{Z}$ is $(-1)^{r_2}$, where $2r_2$ is the number of complex embeddings of K.